[0001] The present invention relates to a method for establishing a common key within a group of subscribers using a publicly known mathematical group and a publicly known element of the group.

Please amend paragraph [0005] as follows:

[0005] A difficulty of the DH-key exchange lies in that Alice does not know whether she actually communicates with Bob or with a cheater. In the IPSec-Standards of the Internet Engineering Task Force (IETF RFC 2412: The OAKLEY Key Determination Protocol), this problem is solved by using public key certificates in which the identity of a subscriber is combined with a public key by a trust center. In this manner, the identity of an interlocutor becomes verifiable.

Page 3, please insert paragraphs [0011.1] and [0011.2] as follows:

--[0011.1] Known from Menezes et al: "Handbook of applied cryptography" 1997 CRC Press. Boca Raton (US) XP002152150 is a method for establishing a common key involving at least three subscribers. In this design approach, a group member (chair) is defined from whom all activities originate. The selection of common key K lies solely with the chair. Subsequently, common key K is sent from the chair to every group member on the basis of the Diffie-Hellman keys determined in pairs, respectively. Thus, common key K is always just as good as it has been selected by the chair.

[0011.2] In Lennon R E et Al: "Cryptographic key distribution using composite keys" Birmingham, Alabama, DEC.3-6, 1978, New York. IEEE, US Vol. CONF. 1978, December 3rd, 1978 (1978-12-03), pp. 26101-26116-6. XP002098158, a key exchange method is described which is limited to two subscribers. In this design approach, each subscriber generates his/her own random number and sends it to the other subscriber in encrypted form. The common key is then determined by each subscriber from the own random number and the encrypted random number received from the other subscriber, using a symmetrical function (EXC-OR).--.

Page 4, before paragraph [0014] please insert the heading --SUMMARY OF THE INVENTION--.

Please amend paragraph [0014] as follows:

[0014] An object of the present invention is to provide a method for generating a common key within a group of at least three subscribers. The intention is for the method to be designed in such a manner that it stands out over the known methods by a small computational outlay and a small communication requirement (few rounds even in the case of many subscribers). At the same time, however, it is intended to have a comparable security standard as the DH method. The method has to be easy to implement. Information on the structure of the group should not be required for carrying out the method.

Page 4, please insert paragraph [0014.1] as follows:

--[0014.1] The present invention provides a method for establishing a common key for a group of at least three subscribers. The method comprises:

generating by each subscriber Ti of the at least three subscribers a respective message Ni = (g^{zi} mod p) from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zi and sending the respective message from the respective subscriber to all other subscribers Tj of the at least three subscribers, each respective random number zi being selected or generated by the respective subscriber Ti;

generating by each subscriber Ti a transmission key k^{ij} from the messages Nj received from the other subscribers Tj, $j \neq i$, and the respective random number zi according to k^{ij}: = Nj^{zi} = $(g^{zj})^{zi}$;

sending by each subscriber Ti the respective random number zi in encrypted form to all other subscribers Tj by generating the message Mij according to Mij := $E(k^{ij}, zi)$, $E(k^{ij}, zi)$ being a symmetrical encryption algorithm in which the data record zi is encrypted with the transmission key k^{ij}; and

determining a common key k by each subscriber Ti using the respective random number zi and the random numbers zj, $j \neq i$, received from the other subscribers according to

$$k: = f(z1, ..., zn),$$

f being a symmetrical function which is invariant under a permutation of its arguments.--.

Before paragraph [0022], please insert the following: the heading --BRIEF DESCRIPTION OF THE DRAWING--; paragraph [0021.1] as follows:

--[0021.1] Fig. 1 shows a flow chart of a method for establishing a common key within a group of subscribers.--;

the heading --DETAILED DESCRIPTION--; and paragraph [0021.2] as follows:

[0021.2] Referring to Fig. 1, in a method according to the present invention for establishing a common key within a group of subscribers, by each subscriber Ti of the at least three subscribers a respective message $Ni = (g^{zi} \bmod p)$ is generated from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zi and the respective message is sent from the respective subscriber to all other subscribers Tj of the at least three subscribers (see block 102). Each respective random number zi is selected or generated by the respective subscriber Ti. Then, by each subscriber Ti a transmission key k^{ij} is generated from the messages Nj received from the other subscribers Tj, $j \neq i$, and the respective random number zi according to $k^{ij} := Nj^{zi} = (g^{zj})^{zi}$ (see block 104). By each subscriber Ti the respective random number zi is sent in encrypted form to all other subscribers Tj by generating the message Mij according to $Mij := E(k^{ij}, zi)$, $E(k^{ij}, zi)$ being a symmetrical encryption algorithm in which the data record zi is encrypted with the transmission key k^{ij} (see block 106). Finally, a common key k is determined by each subscriber Ti using the respective random number zi and the random numbers zj, $j \neq i$, received from the other subscribers according to $k := f(z1, ..., zn)$, f being a symmetrical function which is invariant under a permutation of its arguments (see block 108).--.

Please amend paragraph [0026] as follows:

[0026] A variant of the method is to assign a special role to one of subscribers T1-Tn for the execution of the second method step. If this role is assigned, for example, to subscriber T1, then method steps 2 and 3 or b and c are executed only by subscriber T1. In fourth method step d, all subscribers T1-Tn involved in the method compute common key k according to the assignment $k := h(z1, g^{z2}, ..., g^{zn})$, it being required for (x1, x2, ..., xn) to be a function which is symmetrical in arguments x2, ... xn. This variant drastically reduces the number of messages to be sent. An example of such a function g is, for instance,

$$k := h(z1, g^{z2}, ..., g^{zn}) = g^{z1\,z1} \cdot g^{z2 \cdot z1} \ldots g^{zn\,z1}.$$

Page 9, please delete the heading "METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS".

Page 9, first line change "(2) What is claimed is" to --WHAT IS CLAIMED IS--.